CLAIMS

1. A mutually authenticating method for mutually authenticating a reproducing apparatus and an information processing apparatus, the reproducing apparatus comprising a reproducing portion for reading content information from a recording medium having revocation information and information unique to the recording medium, the revocation information being used to determine whether or not an electronic device is illegal, the reproducing apparatus being configured to transmit and receive the content information to and from the information processing apparatus for processing the content information, the mutually authenticating method comprising the steps of:

causing the reproducing apparatus to determine whether or not the reproducing apparatus itself should be invalidated using information that represents the reproducing apparatus and the revocation information;

causing the information processing apparatus to determine whether or not the information processing apparatus itself should be invalidated using the information that represents the information processing apparatus and the revocation information; and

causing the reproducing apparatus and the information processing apparatus to mutually authenticate each other using both first key

information generated when the determined result at the first determining step does not represent that the reproducing apparatus should be invalidated and second key information generated when the determined result at the second determining step does not represent that information processing apparatus should be invalidated.

2. The mutually authenticating method as set forth in claim 1,

wherein the mutually authenticating step comprises the steps of:

causing the reproducing apparatus to confirm whether or not the information processing apparatus normally operates through the transferring means; and

causing the information processing apparatus to confirm whether or not the reproducing apparatus normally operates through the transferring means.

3. The mutually authenticating method as set forth in claim 2, further comprising the steps of:

causing the reproducing apparatus to generate a random number;

causing the reproducing apparatus to perform a predetermined calculation;

causing the information processing apparatus to generate a random number; and

causing the information processing apparatus to perform a predetermined calculation,

wherein the first confirming step comprises

the steps of:

causing the reproducing apparatus and the information processing apparatus to mutually exchange a first random number generated at the first random number generating step with a second random number generated at the second random number generating step; and

causing the reproducing apparatus to compare the result calculated at the first calculating step using at least the first key information, the first random number, and the second random number, the first random number and the second random number having been mutually exchanged, with the result calculated at the second calculating step using at least the second key information, the first random number, and the second random number, the second key information, the first random number, and the second random number having been transmitted from the information processing apparatus through the transferring means, the first random number and the second random number having been mutually exchanged, and

wherein the second confirming step comprises the steps of:

causing the reproducing apparatus and the information processing apparatus to mutually exchange a third random number generated at the first random number generating step with a fourth random number

generated at the second random number generating step; and

causing the information processing apparatus to compare the result calculated at the first calculating step using at least the first key information, the third random number, and the fourth random number, the first key information, the third random number, and the fourth random number having been transmitted from the reproducing apparatus through the transferring means, the third random number and the fourth random number having been mutually exchanged, with the result calculated at the second calculating step using at least the second key information, the third random number, and the fourth random number, the third random number and the fourth random number having been mutually exchanged.

4. A program for a mutually authenticating method for mutually authenticating a reproducing apparatus and an information processing apparatus, the reproducing apparatus comprising a reproducing portion for reading content information from a recording medium having revocation information and information unique to the recording medium, the revocation information being used to determine whether or not an electronic device is illegal, the reproducing apparatus being configured to transmit and receive the content information to and from the information processing apparatus for

processing the content information, the mutually authenticating method comprising the steps of:

causing the reproducing apparatus to determine whether or not the reproducing apparatus itself should be invalidated using information that represents the reproducing apparatus and the revocation information;

causing the information processing apparatus to determine whether or not the information processing apparatus itself should be invalidated using the information that represents the information processing apparatus and the revocation information; and

causing the reproducing apparatus and the information processing apparatus to mutually authenticate each other using both first key information generated when the determined result at the first determining step does not represent that the reproducing apparatus should be invalidated and second key information generated when the determined result at the second determining step does not represent that information processing apparatus should be invalidated.

5. A recording medium on which a program for a mutually authenticating method is stored, the mutually authenticating method being adapted for mutually authenticating a reproducing apparatus and an information processing apparatus, the reproducing apparatus comprising a reproducing portion for reading

content information from a recording medium having revocation information and information unique to the recording medium, the revocation information being used to determine whether or not an electronic device is illegal, the reproducing apparatus being configured to transmit and receive the content information to and from the information processing apparatus for processing the content information, the mutually authenticating method comprising the steps of:

causing the reproducing apparatus to determine whether or not the reproducing apparatus itself should be invalidated using information that represents the reproducing apparatus and the revocation information;

causing the information processing apparatus to determine whether or not the information processing apparatus itself should be invalidated using the information that represents the information processing apparatus and the revocation information; and

causing the reproducing apparatus and the information processing apparatus to mutually authenticate each other using both first key information generated when the determined result at the first determining step does not represent that the reproducing apparatus should be invalidated and second key information generated when the determined result at the second determining step does not represent that

information processing apparatus should be invalidated.

6. A signal processing system comprising a reproducing apparatus and an information processing apparatus, the reproducing apparatus comprising a reproducing portion for reading content information from a recording medium having revocation information and information unique to the recording medium, the revocation information being used to determine whether or not an electronic device is illegal, the reproducing apparatus being configured to transmit and receive the content information to and from the information processing apparatus for processing the content information,

wherein the reproducing apparatus further comprises:

first determining means for determining whether or not the reproducing apparatus itself should be invalidated using information that represents the reproducing apparatus and the revocation information,

wherein the information processing apparatus comprises:

second determining means for determining whether or not the information processing apparatus itself should be invalidated using the information that represents the information processing apparatus and the revocation information, and

wherein the signal processing system further

comprises:

mutually authenticating means for causing the reproducing apparatus and the information processing apparatus to mutually authenticate each other using both first key information generated when the determined result of the first determining means does not represent that the reproducing apparatus should be invalidated and second key information generated when the determined result of the second determining means does not represent that information processing apparatus should be invalidated; and

common key generating means for generating a common key that is in common with the reproducing apparatus and the information processing apparatus after the mutually authenticating means has mutually authenticated the reproducing apparatus and the information processing apparatus.

7. The signal processing system as set forth in claim 6,

wherein the mutually authenticating means comprises:

first confirming means for confirming whether or not the information processing apparatus normally operates through the transferring means; and

second confirming means for confirming whether or not the reproducing apparatus normally operates through the transferring means.

8. The signal processing system as set forth in claim 7,

wherein the reproducing apparatus further comprises:

first random number generating means for generating a random number; and

first calculating means for performing a predetermined calculation,

wherein the information processing apparatus further comprises:

second random number generating means for generating a random number; and

second calculating means for performing a predetermined calculation,

wherein the first confirming means comprises:

first random number exchanging means for mutually exchanging a first random number generated by the first random number generating means with a second random number generated by the second random number generating means between the reproducing apparatus and the information processing apparatus; and

first comparing means for comparing the result calculated by the first calculating means of the reproducing apparatus using at least the first key information, the first random number, and the second random number, the first random number and the second random number having been mutually exchanged, with the

result calculated by the second calculating means of the information processing apparatus using at least the second key information, the first random number, and the second random number, the second key information, the first random number, and the second random number having been transmitted from the information processing apparatus through the transferring means, the first random number and the second random number having been mutually exchanged, and

wherein the second confirming means comprises:

second random number exchanging means for mutually exchanging a third random number generated by the first random number generating means with a fourth random number generated by the second random number generating means; and

second comparing means for comparing the result calculated by the first calculating means of the reproducing apparatus using at least the first key information, the third random number, and the fourth random number, the first key information, the third random number, and the fourth random number having been transmitted from the reproducing apparatus through the transferring means, the third random number and the fourth random number having been mutually exchanged, with the result calculated by the second calculating means of the information processing apparatus using at

least the second key information, the third random number, and the fourth random number, the third random number and the fourth random number having been mutually exchanged.

9. The signal processing system as set forth in claim 8,

wherein the common key generating means comprises:

third random number exchanging means for mutually exchanging a fifth random number generated by the first random number generating means with a sixth random number generated by the second random number generating means between the reproducing apparatus and the information processing apparatus;

first common key generating means for generating the common key for the reproducing apparatus using at least the first key information, the fifth random number, and the sixth random number; and

second common key generating means for generating the common key for the information processing apparatus using at least the second key information, the fifth random number, and the sixth random number.

10. The signal processing system as set forth in claim 9, further comprising:

first transmitting means for transmitting information from the reproducing apparatus to the

information processing apparatus through the transferring means in accordance with a common key encrypting system using the common key,

wherein the reproducing apparatus further comprises;

intermediate key information generating means for generating key information unique to the recording medium using the first key information and the information unique to the recording medium.

11. The signal processing system as set forth in claim 10, further comprising:

key information encrypting means for encrypting third key information using at least the key information unique to the recording medium;

encryption key information recording means for recording the third key information encrypted by the key information encrypting means to the recording medium;

final encryption key generating means for generating a content information encryption key in accordance with the third key information; and

content information recording means for recording content information encrypted using the content information encryption key to the recording medium.

12. The signal processing system as set forth in claim 11,

wherein the information processing apparatus comprises the key information encrypting means, the encryption key information recording means, the final encryption key generating means, and the content information recording means, and

wherein the first transmitting means is configured to transmit the key information unique to the recording medium to the information processing apparatus.

13. The signal processing system as set forth in claim 12,

wherein the third key information is key information in accordance with a seventh random number generated by the first random number generating means of the reproducing apparatus, and

wherein the first transmitting means is configured to transmit the third key information to the information processing apparatus.

14. The signal processing system as set forth in claim 12,

wherein the third key information is key information in accordance with an eighth random number generated by the second random number generating means of the information processing apparatus.

15. The signal processing system as set forth in claim 11,

wherein the information processing apparatus

comprises the key information encrypting means, the encryption key information recording means, and the content information recording means,

wherein the first transmitting means is configured to transmit the key information unique to the recording medium to the information processing apparatus,

wherein the reproducing apparatus comprises the final encryption key generating means,

wherein the first transmitting means is configured to transmit the content information encryption key generated by the final encryption key generating means to the information processing apparatus.

16. The signal processing system as set forth in claim 15,

wherein the third key information is key information in accordance with a ninth random number generated by the first random number generating means of the reproducing apparatus.

17. The signal processing system as set forth in claim 15

wherein the third key information is key information in accordance with a tenth random number generated by the second random number generating means of the information processing apparatus, and

wherein the signal processing system further

comprises:

second transmitting means for transmitting information from the information processing apparatus to the final encryption key generating means of the reproducing apparatus through the transferring means in accordance with the common key encrypting system using the common key.

18. The signal processing apparatus as set forth in claim 10, further comprising:

key information decrypting means for decrypting fourth key information that has been encrypted and read from the recording medium using at least the key information unique to the recording medium;

final decryption key generating means for generating content information decryption key in accordance with the fourth key information; and

content information decrypting means for decrypting the content information using the content information decryption key.

19. The signal processing system as set forth in claim 18,

wherein the information processing apparatus comprises the final decryption key generating means and the content information decrypting means.

20. The signal processing system as set forth in claim 19,

wherein the information processing apparatus comprises the key information decrypting means, and

wherein the first transmitting means is configured to transmit the key information unique to the recording medium to the information processing apparatus.

21. The signal processing system as set forth in claim 19,

wherein the reproducing apparatus comprises the key information decrypting means, and

wherein the first transmitting means is configured to transmit the decrypted fourth key information to the information processing apparatus.

22. The signal processing system as set forth in claim 18,

wherein the reproducing apparatus comprises the final decryption key generating means.

23. The signal processing system as set forth in claim 22,

wherein the reproducing apparatus comprises the key information decrypting means, and

wherein the first transmitting means is configured to transmit the content information decryption key generated by the reproducing apparatus to the information processing apparatus.

24. A reproducing apparatus for a signal processing system, the reproducing apparatus comprising

a reproducing portion for reading content information from a recording medium having revocation information and information unique to the recording medium, the revocation information being used to determine whether or not an electronic device is illegal, the reproducing apparatus being configured to transmit the content information to an information processing apparatus for processing the content information,

wherein the reproducing apparatus further comprises:

first determining means for determining whether or not the reproducing apparatus itself should be invalidated using information that represents the reproducing apparatus and the revocation information;

mutually authenticating means for mutually authenticating the information processing apparatus using both first key information generated when the determined result of the first determining means does not represent that the reproducing apparatus should be invalidated and second key information generated when the determined result of a second determining means does not represent that information processing apparatus should be invalidated; and

common key generating means for generating a common key that is in common with the information processing apparatus after the mutually authenticating means has mutually authenticated the information

processing apparatus.

25. An information processing apparatus for receiving content information from a reproducing apparatus through transferring means, the content information being read from a recording medium having revocation information and information unique to the recording medium, the revocation information being used to determine whether or not an electronic device is illegal, the information processing apparatus being configured to process the content information, the information processing apparatus comprising:

second determining means for determining whether or not the information processing apparatus itself should be invalidated using first key information, information that represents the information processing apparatus, and the revocation information, the first key information being generated when a determined result of first determining means of the reproducing apparatus does not represent that the reproducing apparatus itself should be invalidated using information that represents the reproducing apparatus and the revocation information;

mutually authenticating means for mutually authenticating the reproducing apparatus using both the first key information and second key information generated when the determined result of the second determining means does not represent that information

processing apparatus itself should be invalidated; and

common key generating means for generating a common key that is in common with the reproducing apparatus after the mutually authenticating means has mutually authenticated the reproducing apparatus.